

Modifications on Character Sequences and Construction of Large Even Length Binary Sequences

Tingyao Xiong*
xiongtin@msu.edu

and

Jonathan I. Hall†
jhall@math.msu.edu

Abstract

It has been noticed that all the known binary sequences having the asymptotic merit factor ≥ 6 are the modifications to the real primitive characters. In this paper, we give a new modification of the character sequences at length $N = p_1 p_2 \dots p_r$, where p_i 's are distinct odd primes and r is finite. Based on these new modifications, for $N = p_1 p_2 \dots p_r$ with p_i 's distinct odd primes, we can construct a binary sequence of length $2N$ with asymptotic merit factor 6.0.

Keywords: aperiodic correlation, merit factor, primitive characters

1 Introduction

Let $x = (x_0, x_1, \dots, x_{N-1})$ and $y = (y_0, y_1, \dots, y_{N-1})$ (not necessarily binary) be sequences of length N . The *aperiodic crosscorrelation* function between x and y at shift i is defined to be

$$A_{x,y}(i) = \sum_{j=0}^{N-i-1} x_j y_{j+i}, \quad 1 \leq i \leq N-1. \quad (1)$$

When $x = y$, denote

$$A_x(i) = A_{x,x}(i) = \sum_{j=0}^{N-i-1} x_j x_{j+i}, \quad 1 \leq i \leq N-1, \quad (2)$$

the *aperiodic autocorrelation* function of x at shift i .

The *periodic crosscorrelation* function between x and y at shift i is defined to be

$$P_{x,y}(i) = \sum_{j=0}^{N-1} x_j y_{j+i}, \quad 0 \leq i \leq N-1, \quad (3)$$

where all the subscripts are taken modulo N . Similarly, when $x = y$, put

$$P_x(i) = P_{x,x}(i) = \sum_{j=0}^{N-1} x_j x_{j+i}, \quad 0 \leq i \leq N-1, \quad (4)$$

the *periodic autocorrelation* function of x at shift i where all the subscripts are taken modulo N .

*Partial support provided by the National Science Foundation

†Partial support provided by the Institute for Quantum Sciences at Michigan State University and the National Science Foundation

If the sequence x is binary, which means that all the x_j 's are $+1$ or -1 , the *merit factor* of the sequence x , introduced by Golay [1] in 1977, is defined as

$$F_x = \frac{N^2}{2 \sum_{i=1}^{N-1} A_x^2(i)}. \quad (5)$$

Moreover, for a family of sequences

$$S = \{x^1, x^2, \dots, x^n, \dots\},$$

where for each $i \geq 1$, x^i is a binary sequence of increasing length N_i , if the limit of F_{x^i} exists as i approaches the infinity, we call

$$F = \lim_{i \rightarrow \infty} F_{x^i},$$

the asymptotic merit factor (ASF) of the sequence family S .

Since Golay firstly proposed the concept, the Merit Factor problems have attracted high research passion from mathematicians and engineers despite of the challenge. It is noticeable that all of the sequences with high asymptotic merit factor are derived from the primitive real characters. So first of all, we introduce the real primitive characters.

Definition 1.1 *Given an odd prime p , the real primitive character modulo p is defined as*

$$\chi_p(j) = \begin{cases} +1 & , p \nmid j \text{ and } j \text{ is a square modulo } p, \\ -1 & , p \nmid j \text{ and } j \text{ is a not square modulo } p, \\ 0 & , p \mid j \end{cases}$$

More generally, for an odd number N , where $N = p_1 p_2 \dots p_r$ with $p_1 < p_2 < \dots < p_r$ distinct odd primes, the real primitive characters modulo N take the form as

$$\chi_N(j) = \chi_{p_1}(j) \chi_{p_2}(j) \dots \chi_{p_r}(j) \quad (6)$$

Based on the character sequences, we define Legendre sequences and Jacobi sequences which are binary.

Definition 1.2 *For p an odd prime, a Legendre sequence $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_{p-1})$ of length p is defined by the Legendre symbols*

$$\alpha_j = \left(\frac{j}{p} \right) = \begin{cases} 1, & \text{if } j = 0; \\ \chi_p(j), & \text{if } 1 \leq j \leq p-1 \end{cases} \quad (7)$$

Generally, for $N = p_1 p_2 \dots p_r$, where $p_1 < p_2 < \dots < p_r$ are distinct odd primes. A Jacobi sequence $J = (J_1, J_2, \dots, J_{N-1})$ is defined as

$$J_j = \left(\frac{j}{p_1} \right) \cdot \left(\frac{j}{p_2} \right) \dots \left(\frac{j}{p_r} \right) \quad (8)$$

where (\cdot) is the Legendre symbol as defined in expression (7).

It is clear that the Legendre sequences, Jacobi and Modified Jacobi sequences just put new definitions at the i -th position where $(i, N) > 1$. Readers can find more discussion about the differences and similarity among Legendre sequences, Jacobi or modified Jacobi sequences and character sequences in [17].

Given a sequence $x = (x_0, x_1, \dots, x_{N-1})$ of length N , the periodic rotation

$$x^r = (y_0, y_1, \dots, y_{N-1})$$

of x by a fraction r is defined as

$$y_j = x_{j+[Nr]} \pmod{N}, \quad 0 \leq j < N. \quad (9)$$

We define function

$$F_r = \frac{2}{3} - 4|r| + 8r^2, \quad \text{for real } r \text{ with } |r| \leq \frac{1}{2}. \quad (10)$$

Families of sequences	Length	Condition	Source
Legendre sequence	$N = p_1$	$p_1 \rightarrow \infty$	[3]
Modified Jacobi sequence	$N = p_1 p_2$	$\frac{N^{\frac{1}{3}}}{p_1} \rightarrow 0$	[4], [5], [9], [17]
Character sequences	$N = p_1 p_2 \dots p_k$	$\frac{(\log N)^2}{p_1} \rightarrow 0$	[5], [9]

Table 1: Summary of sequence families with high asymptotic merit factor values.

After 1980's, mathematicians have obtained a series of important results about the upper bound of asymptotic merit factors of binary sequences. In Table 1, we list all of known families of sequences with asymptotic merit factor form $\frac{1}{F_r}$. Note that for all the sequences listed in Table 1, 6.0, the best theoretical proven value for the asymptotic merit factor, occurs at the rotation fraction $r = \frac{1}{4}$.

Specifically, at length $N = p_1 p_2$ with $p_1 < p_2$ distinct odd primes, the authors and Jedwab and Schmidt have proved independently that any binary completion of the character sequence has the same asymptotic merit factor form $\frac{1}{F_r}$ under some restriction on p_1 and p_2 values. While Jedwab and Schmidt give a better condition on p_1 and p_2 values as shown in Table 1. Therefore, we have

$$\limsup_{n \rightarrow \infty} F_n \geq 6.0$$

where F_n denotes the maximum value of the merit factor of all the binary sequences of length n . It has been observed [6] that $\limsup_{n \rightarrow \infty} F_n \geq 6.34$ by appending a small fraction of a rotated Legendre sequence at an optimal ratio to the end of the rotated sequence itself.

In 2008, inspired by Parker's work, a doubling technique has been used to construct even length sequences with high asymptotic merit factor 6.0 [16], [8], and the merit factor values for all the rotations of these even length sequences are computed in [13].

It is clear now that, without exception, all the known binary sequences with high asymptotic merit factor ≥ 6.0 are derived from the real primitive character sequences. Therefore, the real primitive character sequence χ_N has become (and seems will continue to be at least in the near future) a good candidate to generate sequences with high asymptotic merit factor.

Now suppose we start with the character sequence χ_N , where $N = p_1 p_2 \dots p_r$, p_i 's are distinct odd primes, and r is finite. If we want to construct a new sequence z with high asymptotic merit factor based on χ_N , we need to give the values to the j - positions such that $(j, N) > 1$. Note that the number of j 's such that $(j, N) > 1 = O(N^{\frac{r-1}{r}})$. Such a large amount obviously deserves very careful construction. The main goal of this paper is giving a new construction on these positions where $N = p_1 p_2 \dots p_r$ with r finite. Based on these new constructions, we could apply the doubling technique shown in [16] on z successfully to get a new sequence z' of length $2N$ with the best proven asymptotic merit factor 6.0.

2 Construction

In the rest of the paper, without confusion, we use notations (i, N) or i_N to represent $\gcd(i, N)$. For both A and B positive, $A \ll B$ means that there exists a constant k independent of A and B , such that $|A| < kB$. And we will use the following notations heavily,

Definition 2.1 For n a positive integer, write $n = \prod_{i=1}^r p_i^{\alpha_i}$, where p_i 's are distinct primes. We define $\omega(n) = r$ to be the number of distinct prime divisors of n .

Definition 2.2 Let n be a positive integer, and $f(x)$ be a function. Define

$$\sum_{x=1}^n {}'f(x) = \sum_{\substack{x=1 \\ (x,n)=1}}^n f(x)$$

For example,

$$\sum_{x=1}^4 x^2 = 1^2 + 3^2 = 10.$$

Recall that in [16], we gave the definition of a binary sequence to be symmetric or antisymmetric. For the convenience, we repeat the definition here:

Definition 2.3 For N is odd, a sequence $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_{N-1})$ of length N is symmetric if $\alpha_i = \alpha_{N-i}$, for $1 \leq i \leq N-1$, and antisymmetric if $\alpha_i = -\alpha_{N-i}$, for $1 \leq i \leq N-1$.

One concrete example of a symmetric or antisymmetric sequence is as in the following Lemma ([17], Lemma 3.5):

Lemma 2.4 Let the character sequence χ_N be as defined in expression (6). Then χ_N is symmetric if $N \equiv 1 \pmod{4}$, and antisymmetric if $N \equiv 3 \pmod{4}$.

□

Given a symmetric or antisymmetric sequence, a simple technique of exchanging the symmetric property is shown as following: ([17], Property 3.6)

Property 2.5 Suppose N is odd. For the sequence $\alpha = (\alpha_0, \alpha_1, \dots, \alpha_{N-1})$ of length N , let the sequence $\beta = (\beta_0, \beta_1, \dots, \beta_{N-1})$ with $\beta_j = (-1)^j \alpha_j$. If α is symmetric, then β is antisymmetric, while if α is antisymmetric, then β is symmetric.

□

To simplify the notations, from now on, we define the triple-valued sequence U of length N to be the character sequence

$$U_j = \begin{cases} \chi_N(j) & , j = 1, \dots, N-1; \\ 1 & , j = 0. \end{cases} \quad (11)$$

By Lemma 2.4, it is easy to see that sequence U is symmetric if $N \equiv 1 \pmod{4}$, and antisymmetric if $N \equiv 3 \pmod{4}$.

Before we give the construction to the sequences which will be discussed throughout the whole paper, we study a concrete example.

Example 1 Suppose $N = 3 \times 5 \times 7 = 105$, sequence U of length 105 is as defined in expression (11), and Jacobi sequence J of length 105 is as shown in expression (8). Since we are only interested in the positions j with $(j, N) > 1$. So we only list some positions j with $(j, N) > 1$ of sequences U and J in the Table 2:

Table 2: Comparison between character sequence and Jacobi Sequence at length $N = 105$

position j	3	5	6	7	9	10	12	14	15	...
U_j	0	0	0	0	0	0	0	0	0	...
J_j	1	1	-1	1	1	-1	1	1	1	...
	↑	↑	↑	↑	↑	↑	↑	↑	↑	
	$\chi_{35}(1)$	$\chi_{21}(1)$	$\chi_{35}(2)$	$\chi_{15}(1)$	$\chi_{35}(3)$	$\chi_{21}(2)$	$\chi_{35}(4)$	$\chi_{15}(2)$	$\chi_7(1)$...

position j	...	90	91	93	95	96	98	99	100	102
U_j	...	0	0	0	0	0	0	0	0	0
J_j	...	-1	-1	-1	-1	-1	-1	1	1	-1
		↑	↑	↑	↑	↑	↑	↑	↑	↑
	...	$\chi_7(6)$	$\chi_{15}(13)$	$\chi_{35}(31)$	$\chi_{21}(19)$	$\chi_{35}(32)$	$\chi_{15}(14)$	$\chi_{35}(33)$	$\chi_{21}(20)$	$\chi_{35}(34)$

In Example 1, U is symmetric because $105 \equiv 1 \pmod{4}$. But Jacobi sequence J is neither symmetric nor antisymmetric because as shown above, some positions give subsequences which are antisymmetric. In Table 3, we list the positions which give antisymmetric subsequences within a Jacobi sequence of length $N = 105$.

Table 3: antisymmetric subsequences inside Jacobi sequence J at length $N = 105$

positions	corresponding subsequence
0, 35, 70	$(1, \chi_3(1), \chi_3(2))$
0, 15, 30, ..., 75, 90	$(1, \chi_7(1), \chi_7(2), \dots, \chi_7(5), \chi_7(6))$
0, 7, 14, ..., 91, 98	$(1, \chi_{15}(1), \chi_{15}(2), \dots, \chi_{15}(13), \chi_{15}(14))$
0, 3, 6, ..., 99, 102	$(1, \chi_{35}(1), \chi_{35}(2), \dots, \chi_{35}(33), \chi_{35}(34))$

Table 4: modified subsequences with the same symmetric property as sequence U .

positions	corresponding subsequence
0, 35, 70	$(1, (-1)^1\chi_3(1), (-1)^2\chi_3(2))$
0, 15, 30, ..., 75, 90	$(1, (-1)^1\chi_7(1), (-1)^2\chi_7(2), \dots, (-1)^5\chi_7(5), (-1)^6\chi_7(6))$
0, 7, 14, ..., 91, 98	$(1, (-1)^1\chi_{15}(1), (-1)^2\chi_{15}(2), \dots, (-1)^{13}\chi_{15}(13), (-1)^{14}\chi_{15}(14))$
0, 3, 6, ..., 99, 102	$(1, (-1)^1\chi_{35}(1), (-1)^2\chi_{35}(2), \dots, (-1)^{33}\chi_{35}(33), (-1)^{34}\chi_{35}(34))$

The subsequences listed in Table 3 are all antisymmetric since $d \equiv 3 \pmod{4}$, where $d \in \{3, 7, 15, 35\}$. This is consistent to Lemma 2.4. In the following constructions, we give new definitions on positions j in Table 4. Then the new sequences have the same symmetric property as sequence U .

In Table 4, we change the subsequence $(1, \chi_d(1), \chi_d(2), \dots, \chi_d(d-2), \chi_d(d-1))$ into $(1, (-1)^1\chi_d(1), (-1)^2\chi_d(2), \dots, (-1)^{d-2}\chi_d(d-2), (-1)^{d-1}\chi_d(d-1))$, where $d \in \{3, 7, 15, 35\}$. From Property 2.5, we know that all of the new subsequences become symmetric after the modification. As a result, the new sequence is symmetric, or it has the same symmetric property as sequence U .

We generalize the idea of Example 1 as in the following definitions.

Definition 2.6 Let $N = p_1 p_2 \dots p_r$, where p_i 's are distinct odd primes and $r \geq 2$, for $1 \leq j \leq N-1$, define

$$v_j = \begin{cases} \chi_{N/d}(j/d) & , \text{ if } (j, N) = d > 1 \text{ and } N \equiv N/d \pmod{4} \\ (-1)^{j/d} \chi_{N/d}(j/d) & , \text{ if } (j, N) = d > 1 \text{ and } N \not\equiv N/d \pmod{4} \\ 0 & , \text{ otherwise} \end{cases} \quad (12)$$

and

$$z_j = \begin{cases} 1 & , \text{ if } j = 0; \\ v_j & , \text{ if } (j, N) > 1; \\ U_j & , \text{ otherwise} \end{cases} \quad (13)$$

where U is character sequences defined in expression (11).

The following Lemma shows that the sequence z defined in Definition 2.6 has the same symmetric property as the character sequence U .

Lemma 2.7 Suppose $N = p_1 p_2 \dots p_r$, where p_i 's are distinct odd primes. And the binary sequence z of length N is as defined in Definition 2.6. Then z is symmetric if $N \equiv 1 \pmod{4}$, and z is antisymmetric if $N \equiv 3 \pmod{4}$.

Proof. From Definition 2.6, it is sufficient to show that v as defined in Definition 2.6 above has the same symmetric property as the character sequence U .

By the definition of sequence v , $v_j = 0$ if $(j, N) = 1$. Then $v_{N-j} = 0$ if $(j, N) = 1$. So we only need to consider

v_j values when $(j, N) = d > 1$.

Furthermore, $v_j = \chi_{N/d}(j/d)$ if $N/d \equiv N \pmod{4}$, $v_j = (-1)^{j/d} \chi_{N/d}(j/d)$ if $N/d \not\equiv N \pmod{4}$.

- (1) When $N/d \equiv N \pmod{4}$, Lemma 2.4 shows that $\chi_{N/d}$ has the same symmetric property as character sequence U . Or $\chi_{N/d}$ is symmetric when $N/d \equiv N \equiv 1 \pmod{4}$, and $\chi_{N/d}$ is antisymmetric when $N/d \equiv N \equiv 3 \pmod{4}$.
- (2) When $N/d \not\equiv N \pmod{4}$, again by Lemma 2.4, $\chi_{N/d}$ has the opposite symmetric property to character sequence U . While Property 2.5 shows that $\{(-1)^{j/d} \chi_{N/d}(j/d) \mid j = 0, 1, \dots, N/d - 1\}$ alters the symmetric property of sequence $\chi_{N/d}$.

We combine the discussion above, and we can claim that sequence v has the same symmetric property as the character sequence U . In other words, z is symmetric if $N \equiv 1 \pmod{4}$, and z is antisymmetric if $N \equiv 3 \pmod{4}$. \square

Next we review some definitions from [16].

Definition 2.8 Given two binary sequences $x = (x_0, x_1, \dots, x_{N-1})$ and $e = (e_0, e_1, \dots, e_{N-1})$, we define a new sequence $\{x, x\} = (x_0, x_1, \dots, x_{N-1}, x_0, x_1, \dots, x_{N-1})$ of length $2N$. And we define the product sequence $b = x * e$ by $b_i = x_i e_i$, for $i = 0, 1, \dots, N - 1$.

Definition 2.9 For $\delta = 0, 1$, let the four sequences $\pm e^{(\delta)}$ be given by

$$e_j^{(\delta)} = (-1)^{\binom{j+\delta}{2}} \quad (14)$$

The main goal of this paper is to prove the following theorem.

Theorem 2.10 (main theorem) For any positive integer $r \geq 2$, suppose $N = p_1 p_2 \dots p_r$, where $p_1 < p_2 < \dots < p_r$ are distinct odd primes. Let z be the binary sequences defined in Definitions 2.6, then

- (1) Let F be the asymptotic merit factor of z , f be the offset fraction. Then we have

$$1/F = 2/3 - 4|f| + 8f^2, \quad |f| \leq 1/2, \text{ given}$$

$$\frac{N^\epsilon}{p_1} \rightarrow \infty \text{ for any } \epsilon > 0 \text{ small enough as } N \rightarrow \infty. \quad (15)$$

- (2) Let the sequence e of length $2N$ be one of the four sequences $\pm e^{(\delta)}$ from the Definition 2.9. The new sequence $b = \{z, z\} * e$ of length $2N$ has asymptotic merit factor 6.0 given (15) is satisfied.

The key step of proving Theorem 2.10 is to show that $\sum_{i=1}^{N-1} P_z^2(i) \sim o(N^2)$ when N is large. So we will estimate the periodic autocorrelations of sequence z in the following section.

3 Periodic Autocorrelations of Sequences z

In this section, we will prove that when N is large, $\sum_{i=1}^{N-1} P_z^2(i) \sim o(N^2)$ given condition (15) is held. We will prove this result in three steps.

- (a) In section 3.1, we will prove that $\sum_{i=1}^{N-1} P_U^2(i) \sim o(N^2)$.
- (b) In section 3.2, we will prove that $\sum_{i=1}^{N-1} P_v^2(i) \sim o(N^2)$
- (c) Finally, in in section 3.3, we will prove that $\sum_{i=1}^{N-1} P_z^2(i) \sim o(N^2)$

given condition (15) is satisfied.

3.1 Upper Bound for $\sum_{i=1}^{N-1} P_U^2(i)$.

Firstly, let's review some simple properties from number theory. A well known result about the primitive real characters modulo prime p is as following

Lemma 3.1 Suppose χ_p is as defined in Definition 1.1, then

$$\sum_{n=0}^{p-1} \chi_p(n) \chi_p(n-k) = \begin{cases} p-1 & , \text{ if } p|k; \\ -1 & , \text{ otherwise} \end{cases}$$

Proof. Readers can find the proof to Lemma 3.1 in many references, for instance, Lemma 2 in [18]. \square

Definition 3.2 For an integer n , the divisor function $d(n)$, is defined to be the number of positive divisors of n , or

$$d(n) = \sum_{0 < d|n} 1$$

Definition 3.3 Let $\xi_N^j = e^{\frac{2\pi j}{N}i}$, $u = (u_0, u_1, \dots, u_{N-1})$ be a binary sequence of length N . The Discrete Fourier Transform (D.F.T.) of sequence u is defined as

$$u(\xi_N^j) = \sum_{i=0}^{N-1} u_i \cdot (\xi_N^j)^i.$$

Given a positive integer N , recall that Euler function $\phi(N)$ is defined as the number of i such that $(i, N) = 1$. Then we have

Lemma 3.4 Let $N = p_1 p_2 \dots p_r$, where $p_1 < p_2 < \dots < p_r$ are distinct odd primes. Then

$$N - \phi(N) < r \times \frac{N}{p_1}$$

where $\phi(N) = |\{i | (i, N) = 1\}|$ is the Euler function of N .

Proof.

$$N - \phi(N) < \sum_{i=1}^r (N/p_i - 1) < r \times \frac{N}{p_1}$$

\square

Lemma 3.5 Let y^1, y^2, \dots, y^r be r sequences (not necessarily binary) of length N_1, N_2, \dots, N_r respectively, such that $(N_i, N_j) = 1$ for any $1 \leq i, j \leq r$. Let $N = N_1 \times N_2 \times \dots \times N_r$, define a new sequence $u = y^1 * y^2 * \dots * y^r$ of length N via

$$u_m = \prod_{s=1}^r y_m^s, \text{ where } 0 \leq m \leq N-1.$$

Then the periodic autocorrelations of u is

$$P_u(n) = \prod_{s=1}^r P_{y^s}(n), \text{ where } 0 \leq n \leq N-1.$$

Let $\xi_N^j = e^{\frac{2\pi j}{N}i}$, let $u(\xi_N^j)$ be the D.F.T. as defined in Definition 3.3. Then there exist integers s_1, s_2, \dots, s_r with $(s_i, N_i) = 1$ for $1 \leq i \leq r$, then

$$u(\xi_N^j) = \prod_{i=1}^r y^i(\xi_{N_i}^{js_i})$$

Proof. We will prove the two results simultaneously by the induction on r . When $r = 1$, the result is trivial. Now suppose Lemma 3.5 holds for $r - 1$, where $r \geq 2$ then for r , suppose $y^1, y^2, \dots, y^{r-1}, y^r$ is a series of sequences, where for each i , sequence y^i has length N_i , and $(N_i, N_j) = 1$ for any $1 \leq i < j \leq r$. Now denote $N' = N_1 \times N_2 \cdots \times N_{r-1}$, $u_1 = y^1 * y^2 * \dots * y^{r-1}$, then $u = u_1 * y^r$. By induction,

$$P_u(n) = P_{u_1}(n)P_{y^r}(n)$$

$$u(\xi_N^j) = u_1(\xi_{N'}^{js'}) \times y^r(\xi_{N_r}^{js_r})$$

where $(s', N') = 1$ and $(s_r, N_r) = 1$. Then by induction

$$P_u(n) = P_{u_1}(n)P_{y^r}(n) = \prod_{i=1}^{r-1} P_{y^i}(n) \cdot P_{y^r}(n) = \prod_{i=1}^r P_{y^i}(n)$$

On the other hand, by induction,

$$u_1(\xi_{N'}^{js'}) = \prod_{i=1}^{r-1} y^i(\xi_{N_i}^{js'_i})$$

where $(s'_i, N_i) = 1$, for $i = 1, 2, \dots, r - 1$. Since $(s', N') = 1 \Rightarrow (s', N_i) = 1$, for $i = 1, 2, \dots, r - 1$. Thus $(s's'_i, N_i) = 1$, we denote $s_i = s's'_i$, then

$$u(\xi_N^j) = \prod_{i=1}^{r-1} y^i(\xi_{N_i}^{js_i}) \cdot y^r(\xi_{N_r}^{js_r}) = \prod_{i=1}^r y^i(\xi_{N_i}^{js_i})$$

This finishes the proof of the Lemma. \square

Now we consider a simple example of Lemma 3.5. Let sequence U be as defined in form (11). If $r = 2$, so $N = pq$, where p and q are different odd primes. Then from Lemma 3.1 and 3.5

$$P_U(i) = \begin{cases} 1 - p & , \text{ if } p \mid i \\ 1 - q & , \text{ if } q \mid i \\ +1 & , \text{ otherwise} \end{cases}, \quad \text{where } 1 \leq i \leq N - 1. \quad (16)$$

Generally, for $r \geq 2$ is finite, $N = p_1 p_2 \dots p_r$, where p_i 's are distinct odd primes, we have the following upper estimate for the periodic autocorrelation for U based on Lemma 3.5.

Lemma 3.6 *Let $N = p_1 p_2 \dots p_r$, where $p_1 < p_2 < \dots < p_r$ are distinct odd primes, r is finite. Let the sequence U of entries $\{0, \pm 1\}$ be as defined in form (11), then we have*

$$(a) \quad |P_U(i)| \leq (i, N);$$

$$(b) \quad \sum_{i=1}^{N-1} P_U^2(i) \leq c \frac{N^2}{p_1}, \text{ where } c \text{ is a constant only depends on } r.$$

Proof. For part (a), if $(i, N) = 1$, then $(i, p_j) = 1$ for $j = 1, 2, \dots, r$. From Lemma 3.1 and 3.5,

$$|P_U(i)| = \left| \prod_{j=1}^r P_{\chi_{p_j}}(i) \right| = 1 = (i, N)$$

Now if $(i, N) = N_1 > 1$, then $(i, N/N_1) = 1$. Use the above result and Lemma 3.5,

$$|P_U(i)| = |P_{\chi_{N_1}}(0) \times P_{\chi_{N/N_1}}(i)| = |P_{\chi_{N_1}}(0)| \leq (i, N)$$

So this finishes the proof of part (a).

For part (b), by Lemma 3.5,

$$\begin{aligned}
\sum_{i=1}^{N-1} P_U^2(i) &= \sum_{(i,N)=1} P_U^2(i) + \sum_{(i,N)>1} P_U^2(i) \\
&\leq \sum_{(i,N)=1} \prod_{j=1}^r P_{\chi_{p_j}}^2(i) + \sum_{1 < d|N} \sum_{s=1}^{\frac{N}{d}} P_{\chi_d}^2(sd) P_{\chi_{N/d}}^2(sd) \\
&\leq \sum_{(i,N)=1} 1 + \sum_{1 < d|N} d^2 \cdot \frac{N}{d} \\
&= \phi(N) + \sum_{1 < d|N} N \cdot d \\
&\leq c \frac{N^2}{p_1} \quad \text{where } c \text{ only depends on } r
\end{aligned}$$

where $\phi(N)$ is the Euler function of N . □

So we have proved that $\sum_{i=1}^{N-1} P_U^2(i) \sim O(\frac{N^2}{p_1}) \sim o(N^2)$ given condition (15) is held.

3.2 Upper Bound for $\sum_{i=1}^{N-1} P_v^2(i)$

Before we could give an upper bound of the periodic autocorrelations of sequence v , we still need several properties.

Let $\xi_N^k = e^{\frac{2\pi ki}{N}}$, we have the following lemma

Lemma 3.7 Suppose $N = N_1 \times N_2 \cdots \times N_r$, where $(N_i, N_j) = 1$, for any $1 \leq i < j \leq r$, then for any integer k , there exist integers k_1, k_2, \dots, k_r , such that $(k_i, N_i) = 1$, and

$$\xi_N^k = \prod_{i=1}^r \xi_{N_i}^{kk_i}$$

Proof. We will prove the lemma by induction on r . When $r = 1$, the result is obviously true if we choose $k_1 = 1$. Suppose the result is correct for $r - 1$, where $r \geq 2$. Then for r , so $N = N_1 \times N_2 \cdots \times N_{r-1} \times N_r$, where $(N_i, N_j) = 1$, for any $1 \leq i < j \leq r$. Denote $N' = N_1 \times N_2 \cdots \times N_{r-1}$, so $(N', N_r) = 1$. By induction, there exist integers k' and k_r , with $(k', N') = 1$, $(k_r, N_r) = 1$, such that

$$\xi_N^k = \xi_{N'}^{kk'} \xi_{N_r}^{kk_r} \tag{17}$$

by induction

$$\xi_{N'}^{kk'} = \prod_{i=1}^{r-1} \xi_{N_i}^{kk' s_i}$$

where $(s_i, N_i) = 1$, for $1 \leq i \leq r - 1$. Let $k_i = k' s_i$, then $(k_i, N_i) = 1$, for $1 \leq i \leq r - 1$. Then we have

$$\xi_N^k = \prod_{i=1}^{r-1} \xi_{N_i}^{kk_i} \cdot \xi_{N_r}^{kk_r} = \prod_{i=1}^r \xi_{N_i}^{kk_i}$$

□

Lemma 3.8 Suppose $N = p_1 p_2 \cdots p_r$, where p_i 's are distinct odd primes for $i = 1, 2, \dots, r$. Let χ_N be the primitive character mod N , $f(x)$ be a polynomial of degree k . If for each p_a , $1 \leq a \leq r$, a factorization $f(x) = b(x - x_1)^{d_1} \cdots (x - x_s)^{d_s}$ in \overline{F}_{p_a} , where $x_i \neq x_j$, for $i \neq j$ with

$$(p_a - 1, d_1, \dots, d_s) = 1.$$

Then

$$\left| \sum_{u < n \leq u+t} \chi_N(f(n)) \right| < 2k^r N^{\frac{1}{2}} \log(N)$$

where u and t are integers and $0 < t < N$.

Proof. From the Lemma 3 in [14] (Page 374), we know that for each p_j , $1 \leq j \leq r$,

$$\left| \sum_{x \in F_{p_j}} \chi_{p_j}(f(x)) e^{\frac{2b\pi}{p_j}i} \right| \leq kp_j^{\frac{1}{2}} \quad (18)$$

for any $b \in \mathbb{Z}$. At the same time, one form of the Erdős-Turán inequality ([14] Lemma 4, Page 375) is presented as following

If $m \in \mathbb{N}$, the function $g(x): \mathbb{Z} \rightarrow \mathbb{C}$ is periodic with period m , and u and t are real numbers with $0 \leq t < m$, then

$$\left| \sum_{u < n \leq u+t} g(n) \right| \leq \frac{t+1}{m} \left| \sum_{n=1}^m g(n) \right| + \sum_{1 \leq |h| \leq m/2} |h|^{-1} \left| \sum_{n=1}^m g(n) e^{\frac{h n 2\pi}{m}i} \right| \quad (19)$$

Now apply equation (19) with N and $\chi_N(f(n))$ in place of m and $g(n)$ respectively, and use Lemma 3.5 and equation (18)

$$\begin{aligned} \left| \sum_{u < n \leq u+t} \chi_N(f(n)) \right| &\leq \frac{t+1}{N} \left| \sum_{n=1}^N \chi_N(f(n)) \right| + \sum_{1 \leq |h| \leq N/2} |h|^{-1} \left| \sum_{n=1}^N \chi_N(f(n)) e^{\frac{h n 2\pi}{N}i} \right| \\ &= \frac{t+1}{N} \prod_{j=1}^r \left| \sum_{n=1}^{p_j} \chi_{p_j}(f(n)) \right| + \sum_{1 \leq |h| \leq N/2} |h|^{-1} \prod_{j=1}^r \left| \sum_{n=1}^{p_j} \chi_{p_j}(f(n)) e^{\frac{h k_j n 2\pi}{p_j}i} \right| \end{aligned} \quad (20)$$

where k_j 's are integers such that $(k_j, p_j) = 1$, for $1 \leq j \leq r$.

From expression (18), the first item of (20) satisfies

$$\frac{t+1}{N} \prod_{j=1}^r \left| \sum_{n=1}^{p_j} \chi_{p_j}(f(n)) \right| \leq \frac{t+1}{N} \prod_{j=1}^r kp_j^{\frac{1}{2}} \leq k^r N^{\frac{1}{2}}$$

For the second item in (20), using (18), we have

$$\sum_{1 \leq |h| \leq N/2} |h|^{-1} \prod_{j=1}^r \left| \sum_{n=1}^{p_j} \chi_{p_j}(f(n)) e^{\frac{h k_j n 2\pi}{p_j}i} \right| \leq \sum_{1 \leq |h| \leq N/2} |h|^{-1} k^r N^{\frac{1}{2}}$$

Therefore we obtain

$$\begin{aligned} \left| \sum_{u < n \leq u+t} \chi_N(f(n)) \right| &\leq \frac{t+1}{N} \prod_{j=1}^r \left| \sum_{n=1}^{p_j} \chi_{p_j}(f(n)) \right| + \sum_{1 \leq |h| \leq N/2} |h|^{-1} \prod_{j=1}^r \left| \sum_{n=1}^{p_j} \chi_{p_j}(f(n)) e^{\frac{h k_j n 2\pi}{p_j}i} \right| \\ &\leq k^r N^{\frac{1}{2}} + k^r N^{\frac{1}{2}} \sum_{1 \leq |h| \leq N/2} |h|^{-1} \\ &< 2k^r N^{\frac{1}{2}} \log(N) \end{aligned}$$

which is the desired result we want to prove. \square

Remark 1 In the hypothesis of Lemma 3.8, for each p_j , $1 \leq j \leq r$, $f(x)$ can't be a perfect square over \overline{F}_{p_j} . As an application of Lemma 3.8, the following property gives a general estimate for all $f(x)$ of degree 2.

Property 3.9 Suppose $N = p_1 p_2 \dots p_r$, where p_i 's are distinct odd primes and r is finite. Let χ be the primitive character modulo N . Let u and t be integers such that $0 \leq t < N$, then for any $1 \leq k_1 \neq k_2 \leq N-1$, we have

$$1. |\sum_{u < n \leq u+t} \chi_N(n+k_1)\chi_N(n+k_2)| \ll \max\{d, \sqrt{N/d} \log(N/d)\}$$

$$2. |\sum_{u < n \leq u+t} (-1)^n \chi_N(n+k_1)\chi_N(n+k_2)| \ll \max\{d, \sqrt{N/d} \log(N/d)\}$$

where $d = (k_2 - k_1, N)$.

Proof. We will prove part 1 firstly. For $d = (k_2 - k_1, N)$, write $N = ds$, thus $(k_2 - k_1, s) = 1$, then

$$\begin{aligned} |\sum_{u < n \leq u+t} \chi_N(n+k_1)\chi_N(n+k_2)| &= |\sum_{u+k_1 < n \leq u+t+k_1} \chi_N(n)\chi_N(n+k_2-k_1)| \\ &= |\sum_{u' < n \leq u'+t} \chi_d(n)\chi_s(n)\chi_d(n+k_2-k_1)\chi_s(n+k_2-k_1)| \\ &= |\sum_{u' < n \leq u'+t} \chi_d^2(n)\chi_s(n)\chi_s(n+k_2-k_1)| \quad \text{since } d \mid (k_2 - k_1) \\ &= |\sum_{u' < n \leq u'+t} \chi_s(n)\chi_s(n+k_2-k_1)| \end{aligned}$$

where $u' = u + k_1$. Let $m = \lfloor \frac{t}{s} \rfloor = \lfloor \frac{td}{N} \rfloor \leq d$, since $t < N$.

$$|\sum_{u' < n \leq u'+t} \chi_N(n)\chi_N(n+k_2-k_1)| \leq \sum_{j=1}^m |P_{\chi_s}(k_2-k_1)| + |\sum_{u'+ms < n \leq u'+t} \chi_s(n)\chi_s(n+k_2-k_1)|$$

Because $(k_2 - k_1, s) = 1 \Rightarrow P_{\chi_s}(k_2 - k_1) = -1$, we have

$$\begin{aligned} |\sum_{u'+ms < n \leq u'+t} \chi_s(n)\chi_s(n+k_2-k_1)| &\leq m + |\sum_{u'+ms < n \leq u'+t} \chi_s(n)\chi_s(n+k_2-k_1)| \\ &\leq 2 \cdot \max\{m, 2^{\omega+1} \sqrt{s} \log(s)\} \quad \text{by Lemma 3.8} \\ &\leq 2 \cdot \max\{d, 2^{\omega+1} \sqrt{N/d} \log(N/d)\} \quad \text{since } m \leq d \end{aligned}$$

where $\omega = \omega(s) = \omega(N/d)$ is as defined in Definition 2.1. Therefore,

$$|\sum_{u'+ms < n \leq u'+t} \chi_s(n)\chi_s(n+k_2-k_1)| \ll \max\{d, \sqrt{N/d} \log(N/d)\}$$

For part 2.

$$\begin{aligned} |\sum_{u < n \leq u+t} (-1)^n \chi_N(n+k_1)\chi_N(n+k_2)| &\leq |\sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} (-1)^{2n} \chi_N(2n+k_1)\chi_N(2n+k_2)| \\ &\quad + |\sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} (-1)^{2n-1} \chi_N(2n-1+k_1)\chi_N(2n-1+k_2)| + 2 \\ &\leq |\sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} \chi_N(2n+k_1)\chi_N(2n+k_2)| \\ &\quad + |\sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} \chi_N(2n-1+k_1)\chi_N(2n-1+k_2)| + 2 \end{aligned} \quad (21)$$

For the first item in expression (21), similarly to the above calculation, we have

$$\begin{aligned} |\sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} \chi_N(2n+k_1)\chi_N(2n+k_2)| &= |\sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} \chi_N(n+2^{-1}k_1)\chi_N(n+2^{-1}k_2)| \\ &\ll \max\{d, \sqrt{N/d} \log(N/d)\} \end{aligned} \quad (22)$$

from part 1.

Similarly, from part 1, the second item in expression (21),

$$\begin{aligned} \left| \sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} \chi_N(2n-1+k_1) \chi_N(2n-1+k_2) \right| &= \left| \sum_{\lfloor \frac{u}{2} \rfloor < n \leq \lfloor \frac{u+t}{2} \rfloor} \chi_N(n+2^{-1}(k_1-1)) \chi_N(n+2^{-1}(k_2-1)) \right| \\ &\ll \max\{d, \sqrt{N/d} \log(N/d)\} \end{aligned} \quad (23)$$

Plug the result from expressions (22) and (23) into (21), then we get the result we want to prove. \square

Based on the result of property 3.9, we will give an estimate of the upper bound of the $P_v(i)$, where the sequence v is as defined in Definition 2.6.

Lemma 3.10 *Suppose $N = p_1 p_2 \dots p_r$, where $p_1 < p_2 < \dots < p_r$ are distinct odd primes and $r \geq 2$ is finite. Let ω be the function as defined in Definition 2.1. For each $1 \leq i \leq N-1$, denote $i_N = (i, N)$. Then for the sequence v as defined in Definition 2.6, given condition (15) holds, we have*

$$|P_v(i)| \ll \begin{cases} \sqrt{\frac{N}{p_1 p_2}} \log\left(\frac{N}{p_1 p_2}\right) & , \text{ if } i_N = 1 \\ \frac{i_N}{p_1} & , \text{ if } \omega(i_N) = r-1 \\ \max\{i_N, \sqrt{\frac{N}{i_N}} \log\left(\frac{N}{i_N}\right)\} & , \text{ otherwise} \end{cases} \quad (24)$$

Proof. For any $1 \leq i \leq N-1$, $P_v(i) = \sum_{j=0}^{N-1} v_j v_{j+i}$, while from the definition

$$v_j v_{j+i} \neq 0 \Leftrightarrow (j, N) = m_1 > 1, \text{ and } (j+i, N) = m_2 > 1.$$

Suppose $v_j v_{j+i} \neq 0$, put $(m_1, m_2) = d_1$, then $m_1 = d_1 d_2$, $m_2 = d_1 d_3$, and $d_1 d_2 d_3 | N$. Write $j = k d_1 d_2$, $j+i = s d_1 d_3$, then

$$k d_1 d_2 + i \equiv s d_1 d_3 \pmod{N}, \quad \text{and} \quad \left(k, \frac{N}{d_1 d_2}\right) = \left(s, \frac{N}{d_1 d_3}\right) = 1 \quad (25)$$

Actually, starting with equality (25), we could obtain a series of equalities as following

$$\begin{aligned} (k + d_3) d_1 d_2 + i &\equiv (s + d_2) d_1 d_3 \pmod{N} \\ (k + 2d_3) d_1 d_2 + i &\equiv (s + 2d_2) d_1 d_3 \pmod{N} \\ &\vdots \\ (k + M d_3) d_1 d_2 + i &\equiv (s + M d_2) d_1 d_3 \pmod{N} \end{aligned} \quad (26)$$

where $M = \frac{N}{d_1 d_2 d_3} - 1$.

Denote $(k + n d_3, N/d_1 d_2) = g_1$, and $(s + n d_2, N/d_1 d_3) = g_2$. Then all of the equalities above give us the

following partial sum in P_v .

$$\begin{aligned} & \sum_{n=0}^M v((k+nd_3)d_1d_2)v((s+nd_2)d_1d_3) \\ &= \sum_{\substack{n=0 \\ g_1g_2>1}}^M v((k+nd_3)d_1d_2)v((s+nd_2)d_1d_3) + \sum_{\substack{n=0 \\ g_1=g_2=1}}^M \zeta_n \chi_{\frac{N}{d_1d_2}}(k+nd_3) \chi_{\frac{N}{d_1d_3}}(s+nd_2) \end{aligned} \quad (27)$$

by definition. Where $\zeta_n = \pm 1$ depending on the n values

$$\begin{aligned} & \sum_{\substack{n=0 \\ g_1=g_2=1}}^M \zeta_n \chi_{\frac{N}{d_1d_2}}(k+nd_3) \chi_{\frac{N}{d_1d_3}}(s+nd_2) \\ &= \sum_{n=0}^M \zeta_n \chi_{\frac{N}{d_1d_2d_3}}(k+nd_3) \chi_{d_3}(k+nd_3) \chi_{\frac{N}{d_1d_2d_3}}(s+nd_2) \chi_{d_2}(s+nd_2) \\ &= \sum_{n=0}^M \zeta_n \chi_{\frac{N}{d_1d_2d_3}}(k+nd_3) \chi_{\frac{N}{d_1d_2d_3}}(s+nd_2) \chi_{d_3}(k) \chi_{d_2}(s) \\ &= \chi_{d_3}(k) \chi_{d_2}(s) \chi_{\frac{N}{d_1d_2d_3}}(d_3) \chi_{\frac{N}{d_1d_2d_3}}(d_2) \sum_{n=0}^M \zeta_n \chi_{\frac{N}{d_1d_2d_3}}(kd_3^{-1}+n) \chi_{\frac{N}{d_1d_2d_3}}(sd_2^{-1}+n) \end{aligned}$$

where $d_2d_2^{-1} \equiv d_3d_3^{-1} \equiv 1 \pmod{\frac{N}{d_1d_2d_3}}$. So we have

$$\left| \sum_{\substack{n=0 \\ g_1=g_2=1}}^M \zeta_n \chi_{\frac{N}{d_1d_2}}(k+nd_3) \chi_{\frac{N}{d_1d_3}}(s+nd_2) \right| = \left| \sum_{n=0}^M \zeta_n \chi_{\frac{N}{d_1d_2d_3}}(kd_3^{-1}+n) \chi_{\frac{N}{d_1d_2d_3}}(sd_2^{-1}+n) \right| \quad (28)$$

Now we take a closer look at the ζ_n values. From the Definition 2.6,

1. $\zeta_n = 1$, if $\frac{N}{d_1d_2} \equiv \frac{N}{d_1d_3} \equiv N \pmod{4}$
2. $\zeta_n = (-1)^{(k_n+s_n)}$, if $\frac{N}{d_1d_2} \equiv \frac{N}{d_1d_3} \not\equiv N \pmod{4}$
3. $\zeta_n = (-1)^{k_n}$, $\frac{N}{d_1d_2} \not\equiv N \pmod{4}$, $\frac{N}{d_1d_3} \equiv N \pmod{4}$.
4. $\zeta_n = (-1)^{s_n}$, $\frac{N}{d_1d_3} \not\equiv N \pmod{4}$, $\frac{N}{d_1d_2} \equiv N \pmod{4}$.

where $k_n \equiv k+nd_3 \pmod{\frac{N}{d_1d_2}}$, $s_n \equiv s+nd_2 \pmod{\frac{N}{d_1d_3}}$.

For case 1,

$$\begin{aligned} & \left| \sum_{n=0}^M \zeta_n \chi_{\frac{N}{d_1d_2d_3}}(kd_3^{-1}+n) \chi_{\frac{N}{d_1d_2d_3}}(sd_2^{-1}+n) \right| \\ &= \left| \sum_{n=0}^M \chi_{\frac{N}{d_1d_2d_3}}(kd_3^{-1}+n) \chi_{\frac{N}{d_1d_2d_3}}(sd_2^{-1}+n) \right| \\ &= |P_{\chi_{\frac{N}{d_1d_2d_3}}}(sd_2^{-1}-kd_3^{-1})| \end{aligned} \quad (29)$$

For case 2, suppose n_1 is the first number that $k+n_1d_3 \geq \frac{N}{d_1d_2}$, n_2 is the first number that $s+n_2d_2 \geq \frac{N}{d_1d_3}$. If $n_1 = n_2$, then we still have

$$\left| \sum_{n=0}^M \zeta_n \chi_{\frac{N}{d_1d_2d_3}}(kd_3^{-1}+n) \chi_{\frac{N}{d_1d_2d_3}}(sd_2^{-1}+n) \right| = |P_{\chi_{\frac{N}{d_1d_2d_3}}}(sd_2^{-1}-kd_3^{-1})|$$

So suppose $n_1 \neq n_2$. Without loss, suppose $n_1 < n_2$, noting that all of $d_2, d_3, \frac{N}{d_1 d_2}$ and $\frac{N}{d_1 d_3}$ are odd, then we have

$$\begin{aligned} & \left| \sum_{n=0}^M \zeta_n \chi_{\frac{N}{d_1 d_2 d_3}}(kd_3^{-1} + n) \chi_{\frac{N}{d_1 d_2 d_3}}(sd_2^{-1} + n) \right| \\ & \leq |P_{\chi_{\frac{N}{d_1 d_2 d_3}}}(sd_2^{-1} - kd_3^{-1})| + 2 \left| \sum_{n_1-1 < n \leq n_2-1} \chi_{\frac{N}{d_1 d_2 d_3}}(kd_3^{-1} + n) \chi_{\frac{N}{d_1 d_2 d_3}}(sd_2^{-1} + n) \right| \end{aligned} \quad (30)$$

Since cases 3 and 4 are similar, let's just consider case 3. Then $\zeta_n = (-1)^{k_n}$. Again we let n_1 be the first number that $k + n_1 d_3 \geq \frac{N}{d_1 d_2}$, then we have

$$\begin{aligned} & \left| \sum_{n=0}^M \zeta_n \chi_{\frac{N}{d_1 d_2 d_3}}(kd_3^{-1} + n) \chi_{\frac{N}{d_1 d_2 d_3}}(sd_2^{-1} + n) \right| \\ & = \left| \sum_{0 < n \leq n_1-1} (-1)^n \chi_{\frac{N}{d_1 d_2 d_3}}(n + kd_3^{-1}) \chi_{\frac{N}{d_1 d_2 d_3}}(n + sd_2^{-1}) \right. \\ & \quad \left. - \sum_{n_1-1 < n \leq M} (-1)^n \chi_{\frac{N}{d_1 d_2 d_3}}(n + kd_3^{-1}) \chi_{\frac{N}{d_1 d_2 d_3}}(n + sd_2^{-1}) \right| \\ & \leq \left| \sum_{0 < n \leq n_1-1} (-1)^n \chi_{\frac{N}{d_1 d_2 d_3}}(n + kd_3^{-1}) \chi_{\frac{N}{d_1 d_2 d_3}}(n + sd_2^{-1}) \right| \\ & \quad + \left| \sum_{n_1-1 < n \leq M} (-1)^n \chi_{\frac{N}{d_1 d_2 d_3}}(n + kd_3^{-1}) \chi_{\frac{N}{d_1 d_2 d_3}}(n + sd_2^{-1}) \right| \end{aligned} \quad (31)$$

If $\frac{N}{d_1 d_2 d_3} = 1$, then all of the expressions (29), (30) and (31) are $o(1)$. So suppose $\frac{N}{d_1 d_2 d_3} > 1$.

Put $(i, \frac{N}{d_1 d_2 d_3}) = d$, and $(sd_2^{-1} - kd_3^{-1}, \frac{N}{d_1 d_2 d_3}) = d'$, then we will prove that $d = d'$.

Because $d_2 d_2^{-1} \equiv 1 \pmod{\frac{N}{d_1 d_2 d_3}}$, and $d_3 d_3^{-1} \equiv 1 \pmod{\frac{N}{d_1 d_2 d_3}}$, we suppose $d_2 d_2^{-1} = k_1 \frac{N}{d_1 d_2 d_3} + 1$, and $d_3 d_3^{-1} = k_2 \frac{N}{d_1 d_2 d_3} + 1$ for some integers k_1 and k_2 , then from (25), we have

$$\begin{aligned} (sd_2^{-1} - kd_3^{-1})d_1 d_2 d_3 &= sd_1 d_3 (k_1 \frac{N}{d_1 d_2 d_3} + 1) - kd_1 d_2 (k_2 \frac{N}{d_1 d_2 d_3} + 1) \\ &= \frac{N}{d_1 d_2 d_3} (sk_1 d_1 d_3 - kk_2 d_1 d_2) + (sd_1 d_3 - kd_1 d_2) \\ &\equiv \frac{N}{d_1 d_2 d_3} (sk_1 d_1 d_3 - kk_2 d_1 d_2) + i \pmod{N} \end{aligned}$$

$(i, \frac{N}{d_1 d_2 d_3}) = d \Rightarrow d | \frac{N}{d_1 d_2 d_3} (sk_1 d_1 d_3 - kk_2 d_1 d_2) + i \Rightarrow d | (sd_2^{-1} - kd_3^{-1})d_1 d_2 d_3$, but $(d, d_1 d_2 d_3) = 1 \Rightarrow d | (sd_2^{-1} - kd_3^{-1})$, and $d | \frac{N}{d_1 d_2 d_3}$, therefore, $d | d'$.

On the other hand, $d' | sd_2^{-1} - kd_3^{-1} \Rightarrow d' | \frac{N}{d_1 d_2 d_3} (sk_1 d_1 d_3 - kk_2 d_1 d_2) + i$, and $d' | \frac{N}{d_1 d_2 d_3} \Rightarrow d' | i$, therefore $d' | d$.

So now we have $(i, \frac{N}{d_1 d_2 d_3}) = (sd_2^{-1} - kd_3^{-1}, \frac{N}{d_1 d_2 d_3})$.

Put $(i, \frac{N}{d_1 d_2 d_3}) = i_D \Rightarrow (sd_2^{-1} - kd_3^{-1}, \frac{N}{d_1 d_2 d_3}) = i_D$. By lemma 3.1 and 3.5, expressions (29) satisfies

$$|P_{\chi_{\frac{N}{d_1 d_2 d_3}}}(sd_2^{-1} - kd_3^{-1})| \leq i_D \quad (32)$$

From Property 3.9, equations (30) and (31) satisfy

$$\left| \sum_{n=0}^M \zeta_n \chi_{\frac{N}{d_1 d_2 d_3}}(kd_3^{-1} + n) \chi_{\frac{N}{d_1 d_2 d_3}}(sd_2^{-1} + n) \right| \ll \max\{i_D, \sqrt{\frac{N}{d_1 d_2 d_3 i_D}} \log\left(\frac{N}{d_1 d_2 d_3 i_D}\right)\} \quad (33)$$

where $\omega = \omega(\frac{N}{d_1 d_2 d_3 i_D})$.

If $i_N = 1$, then $i_D = 1$, we want to show that $\omega(d_1 d_2 d_3) \geq 2$. Because if $\omega(d_1 d_2 d_3) = 1$, then $d_1 = p_j$ for some $1 \leq j \leq r$, $d_2 = d_3 = 1$. Then expression (25) becomes

$$kp_j + i \equiv sp_j \pmod{N} \Rightarrow p_j | i \Rightarrow i_N \geq p_j$$

which contradicts to the hypothesis that $i_N = 1$.

If $i_N = i_D = 1$, and $\omega(d_1 d_2 d_3) \geq 2$, then expression (33) satisfies

$$|\sum_{n=0}^M \zeta_n \chi_{\frac{N}{d_1 d_2 d_3}}(kd_3^{-1} + n) \chi_{\frac{N}{d_1 d_2 d_3}}(sd_2^{-1} + n)| \leq 2^{r-2} \sqrt{\frac{N}{p_1 p_2}} \log\left(\frac{N}{p_1 p_2}\right)$$

And $i_N = 1$ implies expression (32)

$$|P_{\chi_{\frac{N}{d_1 d_2 d_3}}}(sd_2^{-1} - kd_3^{-1})| = 1.$$

So we have proved that when $i_N = 1$,

$$|\sum_{\substack{n=0 \\ g_1=g_2=1}}^M \zeta_n \chi_{\frac{N}{d_1 d_2}}(k + nd_3) \chi_{\frac{N}{d_1 d_3}}(s + nd_2)| < 1 + 2^{r-1} \sqrt{\frac{N}{p_1 p_2}} \log\left(\frac{N}{p_1 p_2}\right)$$

Next we want to show that $\omega(i_D) \leq r - 2$. If $\omega(i_D) = r - 1$, then $i_D = N/p_j$, for some $1 \leq j \leq r$, $d_1 = p_j$ and $d_2 = d_3 = 1$. Then equation (25) becomes

$$kp_j + i \equiv sp_j \pmod{N} \Rightarrow p_j | i \Rightarrow N | i$$

it contradicts to the hypothesis that $i < N$. Thus $\omega(i_D) \leq r - 2$.

Now suppose $\omega(i_N) = r - 1$, then from the above statement we have just proved,

$$i_D \leq i_N / p_1$$

use the similar argument to before, expression (32)

$$|P_{\chi_{\frac{N}{d_1 d_2 d_3}}}(sd_2^{-1} - kd_3^{-1})| \leq i_D \leq i_N / p_1,$$

while expression (33)

$$|\sum_{n=0}^M \zeta_n \chi_{\frac{N}{d_1 d_2 d_3}}(kd_3^{-1} + n) \chi_{\frac{N}{d_1 d_2 d_3}}(sd_2^{-1} + n)| \ll \max\{i_D, \sqrt{\frac{N}{d_1 d_2 d_3 i_D}} \log\left(\frac{N}{d_1 d_2 d_3 i_D}\right)\} \ll i_N / p_1$$

where $\omega = \omega(\frac{N}{d_1 d_2 d_3 i_D})$.

Finally, if $1 \leq \omega(i_N) \leq r - 2$, then $i_D \leq i_N$, so equation

$$|P_{\chi_{\frac{N}{d_1 d_2 d_3}}}(sd_2^{-1} - kd_3^{-1})| \leq i_D \leq i_N,$$

equation (33)

$$\begin{aligned} |\sum_{n=0}^M \zeta_n \chi_{\frac{N}{d_1 d_2 d_3}}(kd_3^{-1} + n) \chi_{\frac{N}{d_1 d_2 d_3}}(sd_2^{-1} + n)| &\ll \max\{i_D, \sqrt{\frac{N}{d_1 d_2 d_3 i_D}} \log\left(\frac{N}{d_1 d_2 d_3 i_D}\right)\} \\ &\ll \max\{i_N, \sqrt{\frac{N}{i_N}} \log\left(\frac{N}{i_N}\right)\} \end{aligned}$$

Now for the rest term of expression (27).

$$\sum_{\substack{n=0 \\ g_1 g_2 > 1}}^M v((k + nd_3)d_1 d_2) \cdot v((s + nd_2)d_1 d_3) \neq 0$$

It means that there exist another set of factors d'_1 , d'_2 and d'_3 , with $d'_1 d'_2 d'_3 | N$ such that

$$k' d'_1 d'_2 + i \equiv s' d'_1 d'_3 \pmod{N}$$

where $(k', \frac{N}{d'_1 d'_2}) = (s', \frac{N}{d'_1 d'_3}) = 1$. Then we can set up another series of equalities similar to (26) and obtain the same upper bound as before. Keep doing this, we could come up with the following

$$|P_v(i)| \leq \sum_{1 < d | N} \left| \sum_{n=0}^M \zeta_n \chi_{\frac{N}{d}}(n + k_d) \chi_{\frac{N}{d}}(n + s_d) \right|$$

where $\zeta_n = \{+1, -1\}$ depending on n values, k_d and s_d are some integers depending on the values of d with $(s_d k_d, \frac{N}{d}) = 1$ and $(s_d - k_d, \frac{N}{d}) = (i, \frac{N}{d})$. Noting that

$$d(N) = \sum_{d | N} 1$$

is a finite number only depending on r value, by the discussion above, we have proved the lemma. \square

Now we can prove that $\sum_{i=1}^{N-1} P_v^2(i) \sim O(\frac{N^2}{p_1})$.

Lemma 3.11 Suppose $N = p_1 p_2 \dots p_r$, where $p_1 < p_2 < \dots < p_r$'s are distinct odd primes and r is finite. Let v be the binary sequences of length N as defined in Definition (2.6), then

$$\sum_{i=1}^{N-1} P_v^2(i) \ll N^2 / p_1$$

Proof. Let $i_N = (i, N)$, then we have

$$\sum_{i=1}^{N-1} P_v^2(i) = \sum_{i_N=1} P_v^2(i) + \sum_{\omega(i_N)=r-1} P_v^2(i) + \sum_{1 \leq \omega(i_N) \leq r-2} P_v^2(i)$$

From Lemma 3.10,

$$\sum_{i_N=1} P_v^2(i) \ll N \times \frac{N}{p_1 p_2} \log^2 \left(\frac{N}{p_1 p_2} \right) \ll \frac{N^2}{p_1} \quad (34)$$

$$\sum_{\omega(i_N)=r-1} P_v^2(i) = \sum_{j=1}^r \sum_{s=1}^{p_j-1} P_v^2(s \frac{N}{p_j}) \ll \sum_{j=1}^r \frac{N^2}{p_j^2 p_j} \ll \frac{N^2}{p_1} \quad (35)$$

where ω is the function as in Definition 2.1.

Note that

$$\sum_{1 \leq \omega(i_N) \leq r-2} P_v^2(i) = \sum_{\substack{d | N \\ 1 \leq \omega(d) \leq r-2}} \sum_{m=1}^{N/d} P_v^2(md) \quad (36)$$

$$\begin{aligned} &\ll \sum_{\substack{d | N \\ 1 \leq \omega(d) \leq r-2}} \sum_{m=1}^{N/d} (max\{d, \sqrt{N/d} \log(N/d)\})^2 \\ &\leq \sum_{\substack{d | N \\ 1 \leq \omega(d) \leq r-2}} \frac{N}{d} \cdot (max\{d, \sqrt{N/d} \log(N/d)\})^2 \ll \frac{N^2}{p_1} \end{aligned} \quad (37)$$

The last inequality follows from the fact that r is finite.

Combine the results from equations (34), (35) and (36), we have

$$\sum_{i=1}^{N-1} P_v^2(i) \ll \frac{N^2}{p_1}$$

□

Now we have proved that both $\sum_{i=1}^{N-1} P_U^2(i)$ and $\sum_{i=1}^{N-1} P_v^2(i)$ are $\sim O(\frac{N^2}{p_1})$. In next subsection, we will prove that $\sum_{i=1}^{N-1} P_z^2(i) \sim O(\frac{N^2}{p_1})$.

3.3 Upper Bound for $\sum_{i=1}^{N-1} P_z^2(i)$

We still need one more property before we could prove that $\sum_{i=1}^{N-1} P_z^2(i) \sim O(\frac{N^2}{p_1})$.

Property 3.12 *For any positive integers i , m , and d , if $N = md$, then*

$$d \cdot (i, \frac{N}{d}) = d \cdot (i, m) \geq (i, N)$$

Proof. The result is obvious because

$$(i, N) = (i, md) = (i, m) \cdot (i, d) \text{ and } d \geq (i, d)$$

□

Lemma 3.13 *Suppose $N = p_1 p_2 \dots p_r$, where $p_1 < p_2 < \dots < p_r$'s are distinct odd primes and r is finite. Let z be the binary sequences of length N as defined in Definition (2.6), then*

$$\sum_{i=1}^{N-1} P_z^2(i) \ll N^2/p_1$$

Proof. Let the binary sequence U be as defined in form (11), then $z_j = U_j + v_j$, where sequence v is as defined in Definition 2.6. So

$$\begin{aligned} \sum_{i=1}^{N-1} P_z^2(i) &= \sum_{i=1}^{N-1} \left(\sum_{j=0}^{N-1} z_j z_{j+i} \right)^2 = \sum_{i=1}^{N-1} \left[\sum_{j=0}^{N-1} (U_j + v_j)(U_{j+i} + v_{j+i}) \right]^2 \\ &= \sum_{i=1}^{N-1} [P_U(i) + P_{U,v}(i) + P_{v,U}(i) + P_v(i)]^2 \\ &= \sum_{i=1}^{N-1} P_U^2(i) + \sum_{i=1}^{N-1} P_v^2(i) \\ &\quad + \sum_{i=1}^{N-1} [2P_U(i)P_{U,v}(i) + 2P_U(i)P_{v,U}(i) + 2P_U(i)P_v(i)] \\ &\quad + \sum_{i=1}^{N-1} [2P_v(i)P_{v,U}(i) + 2P_v(i)P_{U,v}(i)] \\ &\quad + \sum_{i=1}^{N-1} [2P_{U,v}(i)P_{v,U}(i) + P_{U,v}^2(i) + P_{v,U}^2(i)] \\ &= A + B + C + D + E \end{aligned} \tag{38}$$

In expression (38), we have separated the summands into five groups. For instance, $B = \sum_{i=1}^{N-1} P_v^2(i)$, and $E = \sum_{i=1}^{N-1} [2P_{U,v}(i)P_{v,U}(i) + P_{U,v}^2(i) + P_{v,U}^2(i)]$. In the following, we will show that the absolute value of every sum from the same group has the same upper bound. To simplify the notation, it should be understood that all of the following statements are valid when p_1 and p_2 's are **large enough**.

For group A, from Lemma 3.6

$$\sum_{i=1}^{N-1} P_U^2(i) \ll N^2/p_1$$

For group B, by Lemma 3.11, we have

$$\sum_{i=1}^{N-1} P_v^2(i) \ll N^2/p_1$$

For group C, every term in this group could be written as

$$\sum_{i=1}^{N-1} P_U(i) \sum_{m=0}^{N-1} v_m \xi_m, \quad \text{where} \quad \xi_m \in \{+1, -1\}.$$

Lemma 3.1, 3.4, 3.5 and Lemma 3.6 give

$$\begin{aligned} \left| \sum_{i=1}^{N-1} P_U(i) \sum_{m=0}^{N-1} v_m \xi_m \right| &\leq rN/p_1 \times \sum_{i=1}^{N-1} |P_U(i)| \\ &= rN/p_1 \times \left[\sum_{i=1}^{N-1} |P_U(i)| + \sum_{\substack{i=1 \\ (i,N)>1}}^{N-1} |P_U(i)| \right] \\ &< rN/p_1 \times \left[N + \sum_{d|N} \sum_{k=1}^{N/d} |P_U(kd)| \right] \\ &\leq rN/p_1 \times \left[N + \sum_{d|N} N/d \times d \right] \\ &\ll N^2/p_1 \end{aligned}$$

Again, the inequality second to the last follows from the fact that $d(N)$ is a finite number.

Now we consider the terms in group E. Since sequence U and v have the same symmetric property as shown in Lemma 2.7, then we have

$$\begin{aligned} \sum_{i=1}^{N-1} P_{U,v}^2(i) &= \sum_{i=1}^{N-1} \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} U_j v_{j+i} U_m v_{m+i} \\ &= \sum_{i=1}^{N-1} \sum_{j=0}^{N-1} U_j v_{j+i} \sum_{m=0}^{N-1} U_{N-m} v_{N-m-i} \\ &= \sum_{i=1}^{N-1} \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} U_j v_{j+i} v_m U_{m+i} = \sum_{i=1}^{N-1} P_{U,v}(i) P_{v,U}(i) \end{aligned} \tag{39}$$

The third equality follow from Lemma 2.7. Similarly we can prove that

$$\sum_{i=1}^{N-1} P_{v,U}^2(i) = \sum_{i=1}^{N-1} P_{U,v}(i) P_{v,U}(i)$$

Therefore for every term in group E, it is enough to estimate the upper bound of $\sum_{i=1}^{N-1} P_{U,v}(i)P_{v,U}(i)$.

$$\begin{aligned}
\sum_{i=1}^{N-1} P_{U,v}(i)P_{v,U}(i) &= \sum_{i=1}^{N-1} \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} U_j v_{j+i} v_m U_{m+i} \\
&= \sum_{i=1}^{N-1} \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} v_j v_m U_{j-i} U_{m+i} \\
&= \chi_N(-1) \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} v_j v_m \left(\sum_{i=1}^{N-1} U_{j-i} U_{-m-i} \right) \\
&= \chi_N(-1) \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} v_j v_m P_U(m+j)
\end{aligned}$$

while

$$\begin{aligned}
\left| \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} v_j v_m P_U(m+j) \right| &= \left| \sum_{s=0}^{N-1} \sum_{j=0}^{N-1} v_j v_{s-j} P_U(s) \right| \quad \text{where } s = m+j \\
&\leq \left| \sum_{\substack{j=0 \\ s=0}}^{N-1} v_j^2 P_U(0) \right| + \left| \sum_{\substack{s=1 \\ (s,N)>1}}^{N-1} P_v(s) P_U(s) \right| + \sum_{s=1}^N |P_v(s)|
\end{aligned}$$

From Lemma 3.4,

$$\left| \sum_{j=0}^{N-1} v_j^2 P_U(0) \right| = N \sum_{j=0}^{N-1} v_j^2 \leq rN \times N/p_1 \ll N^2/p_1 \quad (40)$$

In the proof of Lemma 3.10, we know that when $(s, N) = 1$, $|P_v(s)| \leq 2^{r-2} \sqrt{\frac{N}{p_1 p_2}} \log\left(\frac{N}{p_1 p_2}\right)$, then when $r \geq 2$,

$$\sum_{s=1}^N |P_v(s)| \ll N \times \sqrt{\frac{N}{p_1 p_2}} \log\left(\frac{N}{p_1 p_2}\right) \ll N^2/p_1 \quad (41)$$

We will have to be more careful in estimating $\left| \sum_{(s,N)>1}^{N-1} P_v(s) P_U(s) \right|$, we write

$$\left| \sum_{\substack{s=1 \\ (s,N)>1}}^{N-1} P_v(s) P_U(s) \right| \leq \left| \sum_{\omega((s,N))=r-1} P_v(s) P_U(s) \right| + \left| \sum_{1 \leq \omega((s,N)) \leq r-2} P_v(s) P_U(s) \right| \quad (42)$$

For the first item of equation (42), and by Lemma 3.10, we have

$$\begin{aligned}
\left| \sum_{\omega((s,N))=r-1} P_v(s) P_U(s) \right| &= \left| \sum_{k=1}^r \sum_{m=1}^{p_k-1} P_v(mN/p_k) P_U(mN/p_k) \right| \\
&\leq \sum_{k=1}^r \sum_{m=1}^{p_k-1} |P_v(mN/p_k)| \times |P_U(mN/p_k)| \\
&\leq \sum_{k=1}^r \sum_{m=1}^{p_k-1} \frac{N}{p_1 p_k} \times \frac{N}{p_k} \\
&< \sum_{k=1}^r \frac{N^2}{p_1 p_k} \\
&\ll \frac{N^2}{p_1}
\end{aligned} \quad (43)$$

Now for the second item of equation (42),

$$\begin{aligned}
\left| \sum_{1 \leq \omega((s,N)) \leq r-2} P_v(s) P_U(s) \right| &= \left| \sum_{\substack{d|N \\ 1 \leq \omega(d) \leq r-2}} \sum_{m=1}^{N/d} {}'P_v(md) P_U(md) \right| \\
&\leq \sum_{\substack{d|N \\ 1 \leq \omega(d) \leq r-2}} \sum_{m=1}^{N/d} {}'|P_v(md)| \times |P_U(md)| \\
&\leq \sum_{\substack{d|N \\ 1 \leq \omega(d) \leq r-2}} \sum_{m=1}^{N/d} {}'max\{d, \sqrt{N/d} \cdot \log(N/d)\} \cdot d \\
&\leq \sum_{\substack{d|N \\ 1 \leq \omega(d) \leq r-2}} N/d \cdot max\{d, \sqrt{N/d} \cdot \log(N/d)\} \cdot d \\
&= \sum_{\substack{d|N \\ 1 \leq \omega(d) \leq r-2}} N \cdot max\{d, \sqrt{N/d} \cdot \log(N/d)\} \ll \frac{N^2}{p_1}
\end{aligned} \tag{44}$$

the last inequality follows from the fact that when r is finite,

$$d(N) = \sum_{d|N} 1 \text{ is finite}$$

Now equations (40) and (41),(43) and (44) give us

$$\left| \sum_{i=1}^{N-1} P_{U,v}(i) P_{v,U}(i) \right| = \left| \sum_{i=1}^{N-1} \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} U_j v_{j+i} v_m U_{m+i} \right| = \left| \sum_{j=0}^{N-1} \sum_{m=0}^{N-1} v_j v_m P_U(m+j) \right| \ll \frac{N^2}{p_1}$$

Finally, for the items in group D, we firstly consider $\sum_{i=1}^{N-1} P_v(i) P_{v,U}(i) = \sum_{i=1}^{N-1} P_v(i) \sum_{j=0}^{N-1} v_j U_{j+i}$. We will use the similar method to the proof for Lemma 3.10 to give an upper estimate of $\sum_{j=0}^{N-1} v_j U_{j+i}$.

From Lemma 3.4 and 3.10, we have

$$v_j U_{j+i} \neq 0 \Leftrightarrow (j, N) = d > 1 \text{ and } (j+i, N) = 1$$

Write $j = kd$, $j+i \equiv s \pmod{N}$. So, $(k, N/d) = (s, N) = 1$.

Again, we can set up the following series of equalities, noting that all the values are taken modulo N .

$$\begin{aligned}
kd + i &\equiv s \pmod{N} \\
(k+1)d + i &\equiv s + d \pmod{N} \\
&\vdots \\
&\vdots \\
(k + (M-1))d + i &\equiv s + (M-1)d \pmod{N}
\end{aligned} \tag{45}$$

where $M = \frac{N}{d}$.

The equation series in (45) give the following partial sum of $\sum_{j=0}^{N-1} v_j U_{j+i}$

$$\begin{aligned}
\sum_{m=0}^{M-1} \zeta_m \chi_{\frac{N}{d}}(m) \chi_N(md+i) &= \sum_{m=0}^{M-1} \zeta_m \chi_d(md+i) \chi_{\frac{N}{d}}(m) \chi_{\frac{N}{d}}(md+i) \\
&= \chi_d(i) \chi_{\frac{N}{d}}(d) \sum_{m=0}^{M-1} \zeta_m \chi_{\frac{N}{d}}(m) \chi_{\frac{N}{d}}(m + id^{-1})
\end{aligned}$$

where $\zeta_m = +1$, or $(-1)^{m'}$ with $m' \equiv m \pmod{N/d}$, $dd^{-1} \equiv 1 \pmod{N/d}$. Thus

$$\left| \sum_{m=0}^{M-1} \zeta_m \chi_{\frac{N}{d}}(m) \chi_N(md+i) \right| = \left| \sum_{m=0}^{M-1} \zeta_m \chi_{\frac{N}{d}}(m) \chi_{\frac{N}{d}}(m+id^{-1}) \right|$$

If $\zeta_m = +1$, for $0 \leq m \leq M-1$, then by Lemma 3.10, we have

$$\left| \sum_{m=0}^{M-1} \zeta_m \chi_{\frac{N}{d}}(m) \chi_{\frac{N}{d}}(m+id^{-1}) \right| = |P_{\chi_{\frac{N}{d}}}(id^{-1})| = (id^{-1}, \frac{N}{d}) = (i, \frac{N}{d}) \quad (46)$$

since $(d, \frac{N}{d}) = 1 \Rightarrow (d^{-1}, \frac{N}{d}) = 1 \Rightarrow (id^{-1}, \frac{N}{d}) = (i, \frac{N}{d})$.

If $\zeta_m = (-1)^{m'}$, where $m' \equiv m \pmod{N/d}$, then just repeating the process in expression (31) and using Lemma 3.9, we can obtain

$$\left| \sum_{m=0}^{M-1} (-1)^{m'} \chi_{\frac{N}{d}}(m) \chi_{\frac{N}{d}}(m+id^{-1}) \right| \ll \max\{i_{N/d}, \sqrt{\frac{N/d}{i_{N/d}}} \log\left(\frac{N/d}{i_{N/d}}\right)\}$$

where $i_{N/d} = (i, N/d)$, $\omega = \omega(\frac{N/d}{i_{N/d}})$.

It is obviously true that $i_{N/d} = (i, N/d) \leq (i, N) = i_N$. And from Property 3.12, we know that $\frac{N/d}{i_{N/d}} \leq \frac{N}{i_N}$, therefore we have

$$\left| \sum_{m=0}^{M-1} (-1)^{m'} \chi_{\frac{N}{d}}(m) \chi_{\frac{N}{d}}(m+id^{-1}) \right| \ll \max\{i_N, \sqrt{\frac{N}{i_N}} \log\left(\frac{N}{i_N}\right)\} \quad (47)$$

For the rest items in $\sum_{j=0}^{N-1} v_j U_{j+i}$, we use the similar argument to before. Since $d(i_N)$ is a finite number, we have the following

$$\left| \sum_{j=0}^{N-1} v_j U_{j+i} \right| \ll \max\{i_N, \sqrt{\frac{N}{i_N}} \log\left(\frac{N}{i_N}\right)\} \quad (48)$$

With Lemma 3.10 and expression (48), we can give an upper estimate to the items in group D:

$$\begin{aligned} \left| \sum_{i=1}^{N-1} P_v(i) \left(\sum_{j=0}^{N-1} v_j U_{j+i} \right) \right| &\leq \sum_{i=1}^{N-1} |P_v(i)| \times \left| \sum_{j=0}^{N-1} v_j U_{j+i} \right| \\ &= \sum_{(i,N)=1} |P_v(i)| \times \left| \left(\sum_{j=0}^{N-1} v_j U_{j+i} \right) \right| + \sum_{1 < d|N} \sum_{s=1}^{N/d} |P_v(sd)| \times \left| \left(\sum_{j=0}^{N-1} v_j U_{j+sd} \right) \right| \\ &= \sum_{(i,N)=1} |P_v(i)| \times \left| \left(\sum_{j=0}^{N-1} v_j U_{j+i} \right) \right| \\ &\quad + \sum_{1 < d|N} \sum_{s=1}^{N/d} |P_v(sd)| \times \left| \left(\sum_{j=0}^{N-1} v_j U_{j+sd} \right) \right| \\ &\ll \sum_{(i,N)=1} \frac{N}{\sqrt{p_1 p_2}} \log^2(N) + \sum_{d|N} \sum_{s=1}^{N/d} (\max\{d, \sqrt{\frac{N}{d}} \log\left(\frac{N}{d}\right)\})^2 \quad \text{by (48)} \\ &\leq \frac{N^2}{\sqrt{p_1 p_2}} \log^2(N) + \sum_{d|N} \frac{N}{d} \cdot (\max\{d, \sqrt{\frac{N}{d}} \log\left(\frac{N}{d}\right)\})^2 \\ &\ll \frac{N^2}{p_1} \end{aligned}$$

the last inequality follows from the fact that for each $1 \leq k \leq r$, the number of $d|N$ with $\omega(d) = k$ is finite. Using the similar method to expression (39), it can be shown that $P_v(i)P_{v,U}(i) = P_v(i)P_{U,v}(i)$, for any $i = 1, \dots, N-1$. Then all of the inequalities above will give us the desired result. \square

Now we are ready to prove Theorem 2.10.

4 Proof of Theorem 2.10

Proof. (Theorem 2.10 part(1))

We denote $\xi_N^j = e^{\frac{2\pi j}{N}i}$. For any sequence x of length N , let $x(\xi_N^j)$ be the Discrete Fourier Transform of x as $x(\xi_N^j) = \sum_{k=0}^{N-1} x_k(\xi_N^j)^k$ as in Definition 3.3. Recall that the interpolation formula ([3], (2.5), page162)

$$x(-\xi_N^j) = \frac{2}{N} \sum_{k=0}^{N-1} \frac{\xi_N^k}{\xi_N^k + \xi_N^j} x(\xi_N^k) \quad (49)$$

Then for the sequence z as defined in Definition 2.6, we have

$$z(\xi_N^j) = U(\xi_N^j) + v(\xi_N^j)$$

Note that from Gauss sum, (for instance, [15] page233)

$$|U(\xi_N^j)| = \begin{cases} \sqrt{N}, & \text{if } (j, N) = 1; \\ 0, & \text{otherwise} \end{cases} \quad (50)$$

Therefore, using the interpolation formula (49), we have

$$|U(-\xi_N^j)| = \left| \frac{2}{N} \sum_{k=0}^{N-1} \frac{\xi_N^k}{\xi_N^k + \xi_N^j} U(\xi_N^k) \right| \leq \frac{2}{\sqrt{N}} \sum_{k=0}^{N-1} \left| \frac{\xi_N^k}{\xi_N^k + \xi_N^j} \right| \leq 2\sqrt{N} \log N \quad (51)$$

Now consider $v(\xi_N^j)$. By definition

$$v(\xi_N^j) = \sum_{\substack{d|N \\ d \equiv N \pmod{4}}} \chi_d(\xi_d^j) + \sum_{\substack{d|N \\ d \not\equiv N \pmod{4}}} \chi_d(-\xi_d^j)$$

Using the result of Gauss sum

$$\left| \sum_{\substack{d|N \\ d \equiv N \pmod{4}}} \chi_d(\xi_d^j) \right| \leq \sum_{\substack{d|N \\ d \equiv N \pmod{4}}} |\chi_d(\xi_d^j)| \ll \sqrt{\frac{N}{p_1}}$$

Doing similar calculation to (51), we have

$$\left| \sum_{\substack{d|N \\ d \not\equiv N \pmod{4}}} \chi_d(-\xi_d^j) \right| \leq \sum_{\substack{d|N \\ d \not\equiv N \pmod{4}}} |\chi_d(-\xi_d^j)| \ll \sqrt{\frac{N}{p_1}} \log\left(\frac{N}{p_1}\right)$$

Then we have obtained

$$v(\xi_N^j) \ll \sqrt{\frac{N}{p_1}} \log\left(\frac{N}{p_1}\right) \quad (52)$$

Note that

$$|v(-\xi_N^j)| \leq \sum_{\substack{d|N \\ d \equiv N \pmod{4}}} |\chi_d(-\xi_d^j)| + \sum_{\substack{d|N \\ d \not\equiv N \pmod{4}}} |\chi_d(\xi_d^j)|$$

Then using exactly the same method, we can have

$$|v(-\xi_N^j)| \ll \sqrt{\frac{N}{p_1}} \log\left(\frac{N}{p_1}\right) \quad (53)$$

Let \tilde{F} be the merit factor of U . Then by Theorem 1.2 of [5] (P35), when condition (??) is satisfied,

$$\lim_{N \rightarrow \infty} \frac{1}{\tilde{F}} = \lim_{N \rightarrow \infty} \frac{1}{2N^3} \sum_{j=0}^{N-1} [|U[\xi_N^j]|^4 + |U[-\xi_N^j]|^4] - 1 = \frac{2}{3} - 4|f| + 8f^2$$

where $f = \lfloor \frac{t}{N} \rfloor$ is the offset fraction.

Now let F be the merit factor of sequence z , then from ([3], (5.4) and (5.7), P624),

$$1/F = \frac{1}{2N^3} \sum_{j=0}^{N-1} [|z(\xi_N^j)|^4 + |z(-\xi_N^j)|^4] - 1$$

Let $1/F - 1/\tilde{F} = G/2N^3$, Our goal is to prove that the limit of F takes exactly the same form as \tilde{F} . In other words,

$$\lim_{N \rightarrow \infty} \frac{1}{F} = \frac{2}{3} - 4|f| + 8f^2$$

provided condition (15) is satisfied, where $f = \lfloor \frac{t}{N} \rfloor$ is the offset fraction. So it suffices to prove that

$$G/2N^3 \rightarrow 0 \quad \text{as } N \rightarrow \infty.$$

To shorten the notation, put $a_j = v(\xi_N^j)$ and $b_j = v(-\xi_N^j)$, then using the form ([3], (5.10), P624),

$$\begin{aligned} |G| \leq & \sum_{j=0}^{N-1} [|a_j|^4 + 6|U(\xi_j)|^2|a_j|^2 + 4(|U(\xi_j)|^2 + |a_j|^2)|a_j| \cdot |U(\xi_j)|] \\ & + \sum_{j=0}^{N-1} [|b_j|^4 + 6|U(-\xi_j)|^2|b_j|^2 + 4(|U(-\xi_j)|^2 + |b_j|^2)|b_j| \cdot |U(-\xi_j)|] \end{aligned} \quad (54)$$

Let $|c_j| = \max\{|a_j|, |b_j|\}$, then from expressions (52) and (53), then

$$|c_j| \ll \sqrt{\frac{N}{p_1}} \log\left(\frac{N}{p_1}\right)$$

Let \mathfrak{U}_j be either $U(\xi_j)$ or $U(-\xi_j)$, then by expressions (50) and (51).

$$|\mathfrak{U}_j| \ll \sqrt{N} \log N$$

If we apply the results from (50), (51), (52), and (53) to (54), then we could obtain

$$\begin{aligned}
|G| &\leq 2 \sum_{j=0}^{N-1} [|c_j|^4 + 6|\mathfrak{U}_j|^2 |c_j|^2 + 4(|\mathfrak{U}_j|^2 + |c_j|^2) |c_j| \cdot |\mathfrak{U}_j|] \\
&\ll \sum_{j=0}^{N-1} [|\sqrt{\frac{N}{p_1}} \log(\frac{N}{p_1})|^4 + 6|\sqrt{N} \log N|^2 |\sqrt{\frac{N}{p_1}} \log(\frac{N}{p_1})|^2 \\
&\quad + 4(|\sqrt{N} \log N|^2 + |\sqrt{\frac{N}{p_1}} \log(\frac{N}{p_1})|^2) |\sqrt{\frac{N}{p_1}} \log(\frac{N}{p_1})| \cdot |\sqrt{N} \log N|] \\
&\leq \sum_{j=0}^{N-1} [\frac{N^2}{p_1^2} \log^4(\frac{N}{p_1}) + 6N \log^2 N \cdot \frac{N}{p_1} \log^2(\frac{N}{p_1}) \\
&\quad + 4 \cdot \frac{N^2}{\sqrt{p_1}} \log^4 N + 4 \cdot \frac{N^2}{p_1^{\frac{3}{2}}} \log^4 N] \\
&\ll \frac{N^3}{\sqrt{p_1}} \log^4(N)
\end{aligned} \tag{55}$$

Thus given condition (15) is satisfied, we have

$$\lim_{N \rightarrow \infty} \frac{G}{2N^3} = 0$$

which finishes the proof for part 1 of Theorem 2.10. \square

Before we could prove part (2) of Theorem 2.10, we still need the following lemma ([16], Lemma 2.7 P933)

Lemma 4.1 *Suppose $\alpha = \{\alpha_0, \alpha_1, \dots, \alpha_{N-1}\}$ is a symmetric or antisymmetric binary sequence of odd length N . Let the sequence ϵ of length $2N$ be one of the four sequences $\pm \epsilon^{(\delta)}$ from the definition 2.9. Put $b = \{\alpha, \alpha\} * \epsilon$, then*

$$\sum_{k=1}^{2N-1} A_b^2(k) = N + \sum_{k=1}^{N-1} A_\alpha^2(k) + 2 \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k) A_\alpha(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k)^2.$$

Now we are ready to prove part (2) of Theorem 2.10. \square

Proof. (Theorem 2.10 part(2))

For $N = p_1 p_2 \dots p_r$ is odd, lemma 2.7 shows that sequence z is symmetric or antisymmetric depending the value of $N \pmod{4}$. Thus for

$$b = \{z, z\} * \epsilon$$

Then lemma 4.1 gives

$$\sum_{k=1}^{2N-1} A_b^2(k) = N + \sum_{k=1}^{N-1} A_z^2(k) + 2 \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_z(k) A_z(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_z(k)^2.$$

The proof for part (1) of Theorem 2.10 shows that

$$2 \sum_{k=1}^{N-1} A_z^2(k) \sim O\left(\frac{2}{3} N^2\right) \tag{56}$$

if the condition (15) holds. Lemma 3.13 shows that

$$\sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_z(k)^2 \leq \sum_{k=1}^{N-1} P_z(k)^2 \ll \frac{N^2}{p_1}$$

Then given condition (15), by Cauchy-Schwarz inequality

$$\begin{aligned}
\left| \sum_{\substack{k=1 \\ k \text{ even}}}^{N-1} P_z(k) A_z(k) \right| &\leq \sqrt{\left[\sum_{\substack{k=1 \\ k \text{ even}}}^{N-1} A_z^2(k) \right] \left[\sum_{\substack{k=1 \\ k \text{ even}}}^{N-1} P_z^2(k) \right]} \\
&\leq \sqrt{\left[\sum_{k=1}^{N-1} A_z^2(k) \right] \left[\sum_{k=1}^{N-1} P_z^2(k) \right]} \\
&\ll \frac{N^2}{\sqrt{p_1}}
\end{aligned}$$

Therefore, given condition (15) is hold, the asymptotic merit factor of b is

$$\begin{aligned}
\lim_{N \rightarrow \infty} (F_b) &= \lim_{N \rightarrow \infty} \frac{(2N)^2}{2 \left(\sum_{k=1}^{2N-1} A_b^2(k) \right)} \\
&= \lim_{N \rightarrow \infty} \frac{4N^2}{2 \sum_{k=1}^{N-1} A_a^2(k)} \\
&= 4 \times \frac{3}{2} = 6.
\end{aligned}$$

This finishes the proof of part(2) of Theorem 2.10. □

5 Conclusion

For a long time, being afraid of losing ideal properties of the real primitive character sequences, people have been passive in changing the values of those j -th positions with $(j, N) > 1$. However, the authors have shown that we could have more freedom in changing the values on those positions. It could also be possible to construct sequences with asymptotic merit factor exceeding 6.0 by looking at these subtle positions instead of cyclic shifting the sequence and changing the sequence length. The authors wish that this paper could attract further attention to this new direction.

References

- [1] M.J.E. Golay, “Sieves for Low Autocorrelation Binary Sequences”, *IEEE Transactions on Inform. Theory*, vol. 23 no. 1, pp. 43–51, Jan. 1977.
- [2] J. Jedwab, “A Survey of The Merit Factor Problem for Binary Sequences”, *Lecture Notes in Computer Science*, vol. 3486, *Sequences and Their Applications—Proceedings of SETA 2004*, Springer-Verlag, 2005, pp. 30–55.
- [3] T. Høholdt, H.E. Jensen, “Determination of The Merit Factor of Legendre Sequences”, *IEEE Transactions on Inform. Theory*, vol. 34 no. 1, pp. 161–164, Jan. 1988.
- [4] J.M. Jensen, H.E. Jensen, T. Høholdt, “The Merit Factor of Binary Sequences Related to Difference Sets”, *IEEE Transactions on Inform. Theory*, vol. 37 no. 3, pp. 617–625, May 1991.
- [5] P. Borwein, K-K. S. Choi, “Merit Factors of Polynomials Formed by Jacobi Symbols”, *Canad. J. Math.* Vol. 53 (1), 2001 PP.33-50
- [6] P. Borwein, K-K. S. Choi, and J. Jedwab, “Binary Sequences With Merit Factor Greater Than 6.34”, *IEEE Transactions on Inform. Theory*, vol. 50 no. 12, pp. 3234–3249, Dec. 2004.

- [7] M.G. Parker, “ Even Length Binary Sequence Families With Low Negaperiodic Autocorrelation ”, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-14 Proceedings*, Springer-Verlag, (2001), pp.200-210
- [8] N.Y. Yu and G. Gong, “ The Perfect Binary Sequence of Period 4 for Low Periodic and Aperiodic Autocorrelations ”, *Sequences, Subsequences, and Consequences*, Springer-Verlag, Berlin, (2007),37-49
- [9] J. Jedwab, K. Schmidt, “The Merit Factor of Binary Sequences Derived from the Jacobi Symbol”, Preprint, 2010.
- [10] K.U. Schmidt, J. Jedwab, M.G. Parker, “ Two Binary Sequence Families with Large Merit Factor ”, *Advances in Mathematics of Communications*, Volume 3, No.2, 2009, 135-156
- [11] A. Weil, “ Sur les courbes algebriques et les varietes qui s’en deduisent ”, *Actualites Math. Sci.* No.1041(Paris, 1945), Deuxieme Partie, §IV.
- [12] A.A. Karatsuba, “ Sums of Characters With Prime Numbers and Their Applications ”, *Tatra Mt. Math. Publ.* 20 (2000), 155-162.
- [13] W. M. Schmidt, “ Equations over Finite Fields: an elementary approach ”, Springer, 1976
- [14] C. Mauduit and A. Sárközy, “ On Finite Pseudorandom Binary Sequences I: Measure of Pseudorandomness, The Legendre Symbol ”, *Acta Arithmetica*, LXXXII.4 (1997)
- [15] G. Everest, T. Ward, “ An Introduction to Number Theory ”, Springer, 2005.
- [16] T. Xiong and J.I.Hall, “ Construction of Even Length Binary Sequences With Asymptotic Merit Factor 6”, *IEEE Transactions on Information Theory* 54(2): 931-935 (2008)
- [17] T. Xiong and J.I.Hall, “ Modifications of Modified Jacobi Sequences, ” to appear.
- [18] B. Conrey, A. Granville, B. Poonen, K. Soundararajan, “ Zeros Of Fekete Polynomials ”, *Annales de l’institut Fourier*, 50 no. 3 (2000), p. 865-889.

Address:

Department of Mathematics
Michigan State University
East Lansing, MI 48823, U.S.A.